PROTECTING AMERICAN ASSETS -- WHO IS RESPONSIBLE?

by Anthony C. Crescenzi
510 Stewart Drive West
North Syracuse, New York 13212-3414

Executive Summary

Corporate America is facing an international challenge to its intellectual assets and proprietary information. The challenge stems from the economic competition currently dominating the global economy. This competition is an element of international relationships not likely to change in the future. The question is broader than efforts by traditional adversaries to avail themselves of the latest military technology. Historic allies engage in systematic efforts to enhance their economic viability at the expense of American business.

This paper attempts to place the actions of foreign governments utilizing intelligence assets to illicitly acquire US corporate research and development in perspective. This activity has a detrimental effect on the national security of the US. The historical definition of "National Security" requires reevaluation reflecting economic viability as a true measure of national power.

Existing governmental resources are available at minimal cost to provide proactive security countermeasures to industry. To be of value the government must afford these resources to business in a non-burdensome value added manner.

The Challenge Facing Government and Industry

"We are the Federal Bureau of Investigation, not the Federal Bureau of Prevention." This comment was made at a recent Counterintelligence presentation to US Government contractors by a Special Agent of the Federal Bureau of Investigation (FBI). This observation sums up a dilemma currently confronting the Federal Government with respect to its efforts to protect American high technology, intellectual property, and leading edge research and development. Does the government have a role in protecting those assets that ensure US military superiority and commercial success?

Where the information to be protected is classified, programs like the National Industrial Security Program (NISP) are in place to ensure adequate security countermeasures are present. Assistance is provided to government contractors by the Defense Investigative Service (DIS) or other government activities as appropriate. However, a void exists with respect to efforts to provide a similar service for industry's intellectual property, targeted by Foreign Intelligence Services (FISs).

Large corporations are well aware of the competitive threats to their proprietary information and implement security countermeasures to safeguard identified assets. Small to midsize companies lacking professional security staffs are left largely to their own devices in dealing with this threat to their businesses. You could debate the effectiveness of these measures but security professionals unanimously agree that if targeted by a foreign intelligence service corporate resources are inadequate.

Currently business can expect minimal assistance from the US government unless a connection with classified information is present. The FBI is making a solid effort to provide security awareness via their recent ANSIR (Awareness of National Security Issues and Response) Program. This is an expansion of the Defensive Counterintelligence Awareness program (DECA) used for many years to disseminate the counterintelligence message to industry. As presently configured these efforts constitute an effort at security awareness but do not address the proactive implementation of security countermeasures.

A report prepared by the American Society for Industrial Security (ASIS), **ASIS Special Report: Trends in Intellectual Property Loss**[1] identifies and quantifies the foreign sponsored threat to private industry. The survey reports incidents involving sixteen foreign entities eight of which were among twelve nations assessed by the US counterintelligence community as the most actively involved in targeting US interests. Data indicates some foreign companies and governments pose a significant and continuing threat to intellectual property, defined as patents, copyrights, trademarks, and trade secrets. The severity of the problem has also been recognized by Congress. Legislation introduced by Senator Cohen of Maine in January 25, 1996, became law on October 11, 1996. Senator Cohen's comments introducing the bill provide additional insight into the government's perception of this issue.

"It is imperative the United States send a clear message to both our friends and our foes that this country does not accept international state-sponsored economic espionage as a legitimate business practice. We must demonstrate our resolve to combat this unfair economic practice, regardless of who engages in it.

This legislation will fight a practice that is polluting the international free market and robbing our nation's firms and workers of the success they have earned with their technological innovation and marketing know-how."

The National Counterintelligence Center (NACIC) and the US Department of State's Overseas Security Advisory Council (OSAC) conducted a survey in December 1994 to assess the severity of the threat. Fourteen hundred surveys were mailed to corporate security managers. Key findings of the survey highlight the following:[2]

- the mechanisms in place for the exchange and sharing of counterintelligence (CI) information need energizing and improvement, and
- more emphasis is required for awareness training to heighten employee sensitivities to the information collection tactics of foreign governments and the potential for loss's through industrial theft and other illicit practices by foreign interests

Further illustrating the extent and seriousness of the problem is the Central Intelligence Agency (CIA) report issued in May 1996 which for the first time, publicly identified six nations as aggressive collectors of economic information.

The new Economic Espionage legislation will provide enforcement activities like the FBI with an effective tool for investigating and prosecuting instances of economic espionage after they occur. Investigation and prosecution though desirable and necessary do little to prevent the loss of private sector research and development illicitly acquired by foreign interests. The comments by the FBI special agent referring to the Bureau as an "investigative rather than a preventive agency" are particularly insightful. The obvious question is "What proactive measures should be implemented to level the playing field for US industry targeted by the intelligence services of foreign governments"?

Is National Security Involved?

Decision makers in government and industrial leaders need to determine if the government has a role to play in assisting industry in protecting their unclassified research and development. President Clinton's statement on Economic Espionage October 15, 1996 emphasizes that in today's world the economy and national security are incontrovertibly linked, " Trade secrets are an integral part of virtually every sector of our economy and are essential to maintaining the health and competitiveness of critical industries operating in the United States. Economic espionage and trade secret theft threaten our Nation's national security and economic well-being". The President's remarks state that this issue is one of National Security extending outside traditional boundaries.

Perhaps one of the first steps to be considered if the national leadership desires to effectively address this issue is to formalize and verbalize a new definition of National Security with a major emphasis being placed on economic competition. The passage of the Economic Espionage Act of 1996 is an excellent starting point in formally recognizing the serious nature of the threat posed by foreign governments. The US can look to the government of France as an example of one government's attempt to define its national security interests. French criminal law does not limit spying to only military and political matters. Its definition now includes industrial and commercial matters, particularly those dealing with scientific and technological innovations. The concept of a threat to "national defense interests" is replaced by that of a threat to the "fundamental interests of the nation". This includes the environment and essential elements of scientific and economic potential and cultural heritage. The new laws not only provide sanctions for the covert collection of secret information but also "open" intelligence which consists of gathering information that might present a risk to the fundamental interests of the nation, even if each piece of information by itself is not secret.[3] It is not being suggested that the French definition is appropriate for the US but rather to illustrate that traditional definitions of national security based solely on a nations military strength do not portray the competitive nature of the present global economy.

Existing Government Resources

By virtue of its traditional role in the NISP, and its recent efforts to integrate security counter measures with counterintelligence education and awareness DIS is uniquely

positioned to be a key contributor in any program designed to assist industry in protecting assets of national significance. DIS has no role in operational counterintelligence matters. However, its charter as a security countermeasures organization makes it ideally suited to provide industry with a proactive approach to implementing effective countermeasures tailored to the appropriate threat level likely to be encountered. DIS currently has a work force of trained industrial security professionals, a field structure positioned to respond to industry's needs and contacts within the intelligence community facilitating a mutually beneficial relationship with industry.

If the government desires to be effective in assisting industry in protecting unclassified information of value it must accurately ascertain industry's needs. The government must approach industry as a viable consumer of a value added product and offer its services in a rational, threat appropriate, cost effective manner. Attempts to impose a compliance based regulatory program are doomed to fail. Industry has little desire to increase the regulatory burden it currently faces. Incentives must be basic, and obviously motivated by self interest (the desire to protect company assets).

Industry must be convinced that the service afforded by the government will be of value. The first step in this process is to identify key industry requirements. The aforementioned NACIC/OSAC survey identifies corporations' highest priority as information on foreign government targeting of their proprietary information, employees, telecommunications or facilities or more simply stated "threat information". Ensuring the private sector has a clear comprehension of the threat is a must. The ANSIR program is an attempt to provide this knowledge in a generic fashion. Specific threat information presented in a manner that satisfies clearance and classification issues should be the objective. However, the FBI with its primary mission as an operational and investigative one, may not be positioned most effectively to obtain and convey this threat data from the intelligence community. The recent DoD initiatives to integrate counterintelligence with security countermeasures within DIS are proving fruitful and may be worthy of further exploration as an effective means of providing industry with the information it desires.

Senior management officials must recognize the nature of the problem. There must be a clear understanding that the expenditure of additional resources by industry will be minimal. Additionally, management must be able to conceptualize a return on investment that will improve the overall profitability of the business. Finally, industry requires an Economic Espionage security countermeasures methodology which is standardized, understandable, limited in scope and customized to the individual nature of the business.[4]

DIS possesses the expertise and infrastructure to address each of industry's needs. Assuming senior policy makers recognize existing synergies it would not be difficult to broaden the services currently provided by DIS to encompass security education and awareness training to address company intellectual property assets. The ability to obtain and disseminate threat data satisfies two crucial industry requirements. The security countermeasures which DIS overseas in the classified Defense arena can easily be tailored to the protection of intellectual property. DIS assets are an existing force multiplier available for increased exploitation to the ultimate benefit of the nation.

Glossary

ASIS American Society for Industrial Security

ANSER Awareness of National Security Issues and Response

CIA Central Intelligence Agency

CI Counterintelligence

DECA Defensive Counterintelligence Awareness

DIS Defense Investigative Service

DoD Department of Defense

EEA Economic Espionage Act

EE Economic Espionage

FBI Federal Bureau of Investigation

FIS Foreign Intelligence Service

NACIC National Counterintelligence Center

OSAC Overseas Security Advisory Council

---

[1] ASIS, March 1996 report **Trends in Intellectual Property Loss,** prepared by Richard J. Heffernon CCP and Dan T. Swartwood OCP.

[2] 1994 NACIC/OSAC Survey of the Counterintelligence Needs of Prviate Industry.

[3] Intelligence Newsletter & MEDNEWS, 24 March 94, Ru Du Seytier, Paris, France 75002.

[4] Strong, J. Thompson, **Tilting With Machiavelli: Fighting Competitive Espionage in the 1990's,** International Journal of Intelligence and Counterintelligence, pp. 161-174; Volume 7, number 2, Summer 1994. Intel Publishing Group, Inc., Box 188, Stroudsburg PA, 18360.